Draft Minutes
Federal PKI Directory Ad Hoc Minutes
Dec. 8, 2000

The third FPKI directory meeting was held on Dec. 8, 2000 at NIST.

Attendance

Nelson Barry, Energy Dept.
Bill Burr (TWG Chairman), NIST
Daryl Clemons, Fed. Mgt. Serv
Bruce Esposito, Novell
Michael R. Gettes, Georgetown Univ.
Ed Harrington, NEXOR
Skip Hirsh, Certicom
Phil Hunt, TidePoint
Richard Lane, SAIC
Robert Malick, NIH
Gene McDowell, Commerce - NOAA
Tom Murphy, NOAA
Monette Respress, Mitretek
Michael F. Stern, Mitretek
Scott Wycokff, Logicon
Shiraz Bhanji, MITRE
Skip Chapman, Conclusive
Brice Eldrige, Novell
George Fortwentler, HHS
Linda Hancock, TEAM
Nelson Hastings, Tidepoint
Hsiaosu Hsiung, CoCert
Bob Johnson, BAH
Richard Lane, J. G. Van Dyke
John E. Mcclendon, Norbec
Gary Moore, Entrust
Erik Pfeifer , PEC
Scott Scheurich, Comcert
Mick Wiser , SAIC
Shu-jen Chang, NIST

Discussion

Michael Gettes of Georgetown University is participating in the Middleware Architecture Committee for Education (MACE) http://middleware.internet2.edu/MACE/, a part of the Higher Ed, Internet II effort, and he described the approach that they are using to domain component names with traditional X.500 names. Gettes advocates the FPKI community to allow the flexibility of combining DC names with X.500 names in the subjectName field of a certificate, and adopt it in the FPKI directory profile since it supports both naming style. No rule of X.500 or LDAP is violated by this approach. Many of Mihael's ideas are discussed in http://www.georgetown.edu/giia/internet2/ldap-recipe.

The discussion that follows adopts the "LDAP style" of writing names with the most significant name on the right (the "X.500 style" would put the most significant name on the left). We can use either notation to express either traditional X.500 directory names (the most significant part being "c=US") or domain component names (the most significant part being "dc=gov"). An example of a "pure traditional X.500 directory name" (expressed in the LDAP style of writing names) would be:

cn=John Smith, ou=Internal Revenue Service, ou=Department of Treasury, o=U.S. Government, c=US

Based on the equivalent IRS domain name irs.treas.gov, the domain component name then would be:

cn=John Smith, dc=irs, dc=treas, dc=gov

Michael argues that there is no rule in X.500 that prohibits combining DC names with X.500 names. The principal requirement for a distinguished name is for it to be globally unique. Given

that there is no owner of the c=US portion of the directory information tree (and unlikely to be one), DC naming is logical at this time and requires no new registration or management. The combined use of DC names and X.500 names enforces name uniqueness, and may allow directory service discovery via DNS SRV records (http://www.ietf.org/internet-drafts/draft-ietf-ldapext-locate-04.txt).

Some equivalent examples of the combined X.500/DCN names would be:

1. cn=John Smith, dc=irs, dc=treas, dc=gov, ou=Department of Treasury, o=U.S. Government, c=US

2. cn=John Smith, dc=irs, ou=Internal Revenue Service, dc=treas, dc=gov, ou=Department of Treasury, o=U.S. Government, c=US

3. cn=John Smith, ou=Internal Revenue Service, dc=irs, dc=treas, dc=gov, ou=Department of Treasury, o=U.S. Government, c=US

Or, starting with the ".gov" domain name:

4. cn=John Smith, ou=Internal Revenue Service, o=U.S. Government, dc=irs, dc=treas, dc=gov

5. cn=John Smith, ou=Internal Revenue Service, o=U.S. Government, c=US, dc=irs dc=treas, dc=gov

Figure 1 below illustrates the directory structure when the root is o=U.S. Government, c=US. Figure 2 below illustrates the structure when dc=gov is the root.

Michael mentioned a forthcoming Higher Ed letter pointing out the importance of LDAP, XML and DC naming. The letter amplifies points made earlier in an original letter sent to the Federal CIO Council regarding the use of X.509. The intent of all these is, to not only foster the use of the FBCA model, but also help it grow into something more practical outside the US government. New infrastructures are being designed in the Internet2/EDUCAUSE arenas to try and meet the needs of academia, medical schools and a myriad of applications (http://middleware.internet2.edu). Allowing this flexibility to use both DC and X.500 names will facilitate implementations to interoperate between institutions of higher education and the federal government. Recent changes to the FBCA CP will allow for this flexibility as well.

There was an extensive discussion of the proposal. The FBCA would stand up a directory server with 2 (or 3) roots for [o=US Government, c= US], [dc=gov], and, possibly, [dc=mil]. Agencies would be encouraged to include the combined name form in entity certificates and could choose whether to use [o=US Government, c= US] or [dc=gov] as the most significant part of the name. It would also be acceptable to use only one name form or the other, however this might limit the techniques that can be applied to search for certificates.

The WG accepted the proposal as a reasonable basis for interoperable naming.

Several issues were raised. One is, do X.500 DSA products "object" to seeing the "c=" attribute subordinate to the "dc=". Are there other features of this naming scheme that "break" some directory products? What are the rules, if any for formulating the combined names? For example all the names above start (on the right) with either the "c=US" or "dc=gov" attribute and end (on

the left) with the common name. This makes sense intuitively, but does it make any difference to the processing of the name??

Action Items

1. Vendors: Check what features this naming scheme could break existing directory products.
2. All: Explore the impact this naming scheme will make on name constraint.
3. NIST: Revise the directory profile to support this option.

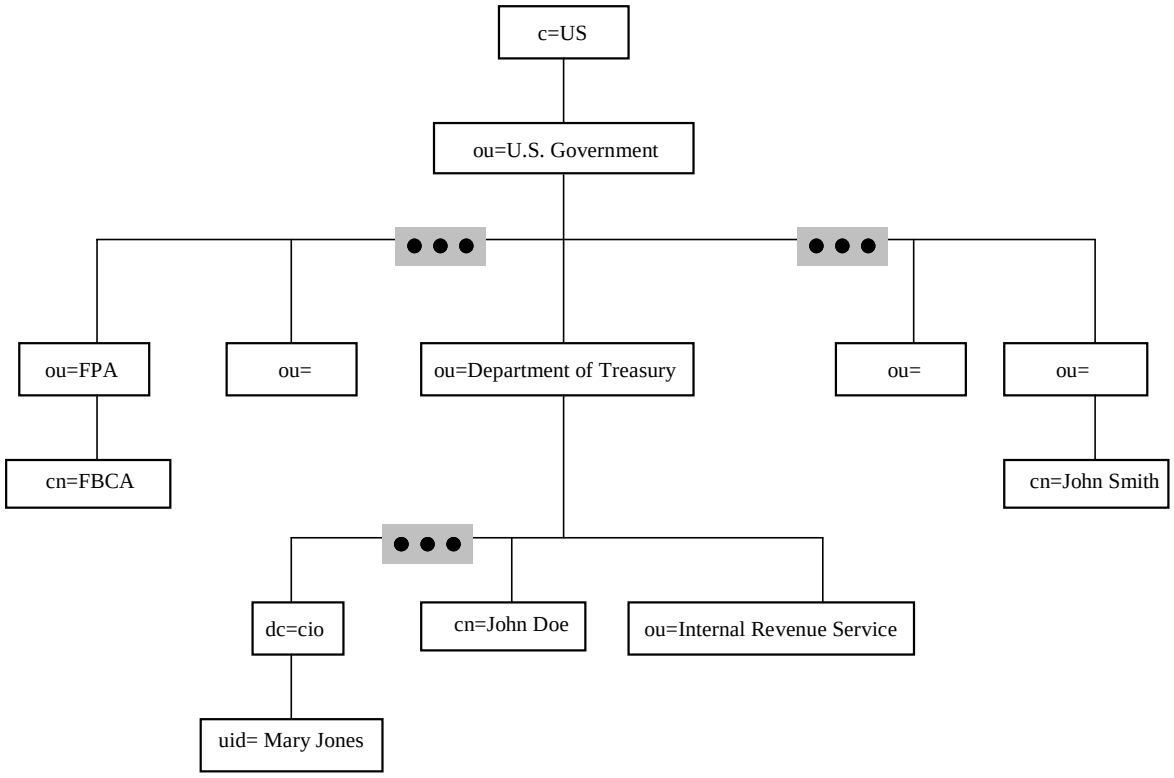

Figure 1.

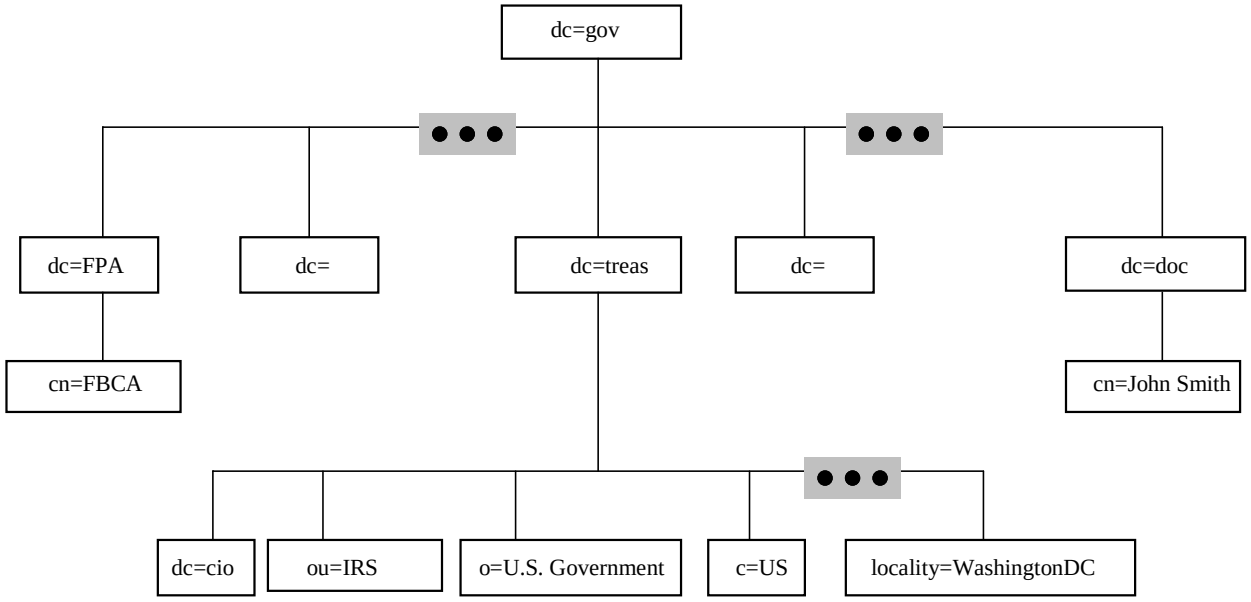

Figure 2.